

---

**EDUCATIONAL TECHNOLOGY  
CONSORTIUM  
COMMUNITY NET  
ACCEPTABLE USE POLICY**

Accepted and Approved by

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

---

# Community Net – EDU VPN

## Acceptable Usage Policy

**Purpose:** This policy guides users of the Community Net (CNET) Education VPN (EDUVPN) Information Technology (IT) infrastructure. It balances the user's ability to benefit fully from information technology with Community Net's need for secure and effectively allocated IT resources.

**Background:** The increasing use of information technology has fundamentally changed the workplace. The Internet, intranets, cellular telephones, fax machines and e-mail have transformed data management and communication and users utilize this valuable resource in many innovative ways.

The networked facility has also created the opportunity to access material and use resources in ways that may not be acceptable. Unacceptable use of information technology could expose the EDUVPN to potential embarrassment and possible litigation. The Educational Technology Consortium (ETC) is empowered to ensuring that this valuable resource is not brought into disrepute through unacceptable use. Users of the EDUVPN are to follow this policy to ensure that their own use of the Community Net's information technology resources is acceptable.

---

**Policy:**

The Infrastructure Sub-Committee of the Educational Technology Consortium has the responsibility of developing and implementing the CNET EDUVPN Acceptable Use Policy.

Users will follow guidelines and policies to enable reasonable and appropriate usage of information systems, and to perform their roles in accordance with all applicable laws, regulations and policies. The ETC will periodically redefine and enhance these guidelines and policies.

This policy addresses circumstances that are new and evolving, or at least unfamiliar. It augments existing user group and Saskatchewan Learning policies.

Users who are found in non-compliance of this policy will be subject to a range of actions up to and including the disconnection of CNET services.

It is the responsibility of the user group Director and/or Director of Education to ensure that any local Acceptable Use Policies do not contravene this policy.

There are three usage types for the EDUVPN infrastructure:

- Acceptable,
- Incidental and
- Unacceptable.

The chart contained in Appendix "J" of this policy provides examples of these three usage types and may be used as a guideline when assessing use of information technology.

The appendices discuss specific applications such as the Internet and e-mail in more detail.

- Appendix 'A' - Internet Use
- Appendix 'B' - E-mail
- Appendix 'C' - Games/Multimedia
- Appendix 'D' - Notebook Computers
- Appendix 'E' - Remote Access Services
- Appendix 'F' - Anti-Virus
- Appendix 'G' - File Sharing
- Appendix 'H' - Collaboration/IP Conferencing Services
- Appendix 'I' - Baseline Connection Requirements

- 
- Appendix 'J' - Acceptable/Incidental/Unacceptable Usages

### **Acceptable**

Acceptable uses are activities required to conduct the businesses of education and libraries. They help fulfill the mandates set forth by School Divisions, Post Secondary Institutions, Libraries and Saskatchewan Learning.

Acceptable use is any application used in the delivery of services by education partners which does not disproportionately consume available resources.

### **Incidental**

Incidental uses are those that are neither explicitly permitted nor explicitly denied. Incidental usage that becomes an imposition on others or burdens systems is no longer incidental, but unacceptable, and is not permitted.

### **Unacceptable**

Unacceptable use impedes the work of others and may unintentionally damage the infrastructure. Unacceptable usage may generate extra costs for CNET and/or its CNET partners.

It is unacceptable to:

- Use, copy, or otherwise access anyone else's files without authorization.
- Use the EDUVPN information technology infrastructure for activities that contravene the law, existing policies or regulations.
- Use any part of the EDU VPN information technology infrastructure for personal financial gain.
- Infringe copyright or proprietary rights.
- Permit unauthorized access.
- Create or propagate computer viruses.
- Damage files, equipment, software, or data belonging to others.
- Use or attempt to use unauthorized access methods or abilities.

- 
- Compromise the privacy of users and their personal data.
  - Damage the integrity of a computer system, or the data or programs stored on a computer system.
  - Bring Community Net into disrepute.
  - Disrupt the intended use of system or network resources.
  - Put unjustifiable demands on Community Net's infrastructure
  - Facilitate unauthorized access attempts on other computer systems.
  - Result in the uploading, downloading, modification, or removal of files on the network for which such action is not authorized.

The above list is not exhaustive.

The EDUVPN infrastructure provides access to outside networks. Users may encounter offensive or objectionable material. The EDUVPN does not assume responsibility for the content of any of these outside networks.

Without specific authorization, users must not cause, permit, or attempt any installation of hardware or software, destruction or modification of data or equipment that will affect other users of the EDUVPN.

**Monitoring:** Users should be aware that computer usage can be traced by site logs and other tracked information. Community Net reserves the right to access the contents of all files stored on its systems and all messages transmitted through its information technology infrastructure.

**Application:** This policy applies to all users who subscribe to services provided through the CNET EDUVPN.

---

## Appendices

*Technology changes rapidly and its use varies widely within Community Net. For example, a few years ago personal digital assistants (PDAs), networked photocopiers and workstations with worldwide Internet access were unheard of. Now, they are becoming commonplace in many offices. The list of applications and devices in these appendices is therefore illustrative, not exhaustive. It represents a baseline for acceptable usage and may be used as a template for CNET EDUVPN-specific policies.*

### Appendix "A"

#### INTERNET USE

Partners who provide access to CNET EDUVPN services including the Internet should be familiar with:

- Copyright laws as they apply to software and electronic forms of information,
- The Canadian Criminal Code  
<http://laws.justice.gc.ca/en/C-46/text.html>
- Applicable libel and slander laws,
- Community Net's Security Policy.
- SANS ([www.sans.org](http://www.sans.org))
- CERT ([www.cert.org](http://www.cert.org))
- Existing user group policies

### Appendix "B"

#### E-MAIL

Users must not attempt to read another person's e-mail unless otherwise authorized. The e-mail system is a function of Community Net EDUVPN. Users should have no reasonable expectation of privacy in e-mail transmitted, received and stored on and/or through the system.

Many users access e-mail through web-based accounts hosted on external commercial sites such as [user@hotmail.com](mailto:user@hotmail.com), [user@msn.com](mailto:user@msn.com), [user@sasktel.net](mailto:user@sasktel.net) or other free/commercial web based e-mail services. If irresponsible use of web-based e-mail compromises Community Net EDUVPN services, permission to access web-based e-mail from within the network will be reviewed on an individual and/or divisional basis.

---

**Appendix "C"****GAMES/MULTIMEDIA:**

- Using the CNET EDUVPN infrastructure to access games or multimedia services for non-educational purposes is an unacceptable use of a valuable resource and is not permitted.

**Appendix "D"****NOTEBOOK COMPUTERS:**

- Notebook computers that have access to CNET must be secured appropriately to prevent a security risk in the event of loss or theft.

**Appendix "E"****REMOTE ACCESS**

- Information regarding remote access to CNET must be held confidential. Remote access instructions, dialup phone numbers and other similar information, must NOT be posted on electronic bulletin boards, listed in telephone directories, or otherwise revealed to unauthorized parties.

**Appendix "F"****ANTI-VIRUS:**

- Users shall not introduce a virus of any type to any CNET EDUVPN computer system. All users are responsible for the protection of computer systems from computer viruses. Individual users must use extreme caution when accessing any external data, diskette, files or programs intended to be stored on Community Net computers.

**Appendix "G"****FILE SHARING:**

- Unauthorized distribution/access of copyrighted works and non-educational material including, but not limited to audio, video or program files through Peer-to-Peer programs (e.g., Kazaa, WinMX, eDonkey, etc.) is not permitted.

---

## **Appendix "H"**

### **COLLABORATION/IP CONFERENCING SERVICES:**

- Users are responsible for the protection of computer systems while using these services. Users must employ caution when utilizing these services for conferences or Remote Control.

## **Appendix "I"**

### **BASELINE CONNECTION REQUIREMENTS:**

- As a condition of connection to Community Net, Users of the EDUVPN are required to ensure that their data networks meet the following minimum requirements:(note: these requirements are subject to change)

#### **Firewalls:**

- All sites connected to CNET must have a firewall in order to protect user networks from attack.

#### **Wireless:**

- Users who implement wireless solutions must ensure that the system is secured from unauthorized access.

#### **Internet Accessible Systems:**

- It is the responsibility of the user group to ensure that all Internet accessible systems are secured against outside attack.
- Typically Internet servers will include mail, web and other public content servers. Mail servers should be securely configured, patches kept current, and must not allow relaying of unauthorized messages. Web servers must be patched appropriately and should be protected from outside attacks.
- All systems that are accessible by outside sources must be secured against the SANS Top 20 list of vulnerabilities (<http://www.sans.org/top20/>).
- Unused services must be disabled on any publicly accessible system.

## Appendix "J"

### ACCEPTABLE/INCIDENTAL/UNACCEPTABLE USAGE

	ACCEPTABLE		INCIDENTAL		UNACCEPTABLE		
	Acceptable	Acceptable/ Incidental	Incidental	Incidental/ Unacceptable	Unacceptable	Unacceptable (contravenes other Policies)*	Illegal
<b>Stand Alone Computer</b>	Word Processing. Doing the budget.		Preparing a roster for your children's soccer team over the lunch hour.	Preparing a roster for your child's soccer team, tying up the computer when co-workers need access.	Crashing the computer by installing a graphics-intensive multi-player combat game.	Excessive personal use of the computer.	Running a pirated version of a popular program on the computer.
<b>Networked Computer</b>	Sending an e-mail to all division technical coordinators with minutes of a meeting.		E-mails to co-workers with birthday wishes, holiday greetings.	Sending Division-wide e-mails with 'puppies 4 sale' type messages.	Distributing chain e-mail with large executable file attachments that waste limited network resources and may contain viruses.	Distributing racist or obscene jokes, pictures or graphics via e-mail.	Making a libelous statement about a co-worker or student in an e-mail.
<b>Networked Computer on the Internet</b>	Researching the latest developments in a topic with a class of students using the Internet.	An e-mail to a colleague deals with work and the schedule for your up-coming hockey tournament.	Browsing a news site during the lunch hour to keep up with world events.	Subscribing to a newsgroup on a government internet account that is of a personal nature.	Downloading a beta version of a program and installing it without authorization. Downloading racist, sexist, or pornographic material	Excessive personal use of work on the Internet.	Downloading, storing distributing and selling child pornography.

**Note:** These are examples only and not exhaustive or inclusive.